REMARKS

This Amendment is responsive to the Office Action mailed on May 20, 2004. Claims 1 and 17 are amended. Claims 10 and 16 are cancelled.

Claims 1-6, 8, 10, 12, 13, 16, and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ellis (US 6,665,869) in view of McRae (US 6,115,079).

Claims 1-3, 7, 9, 11, 14, 15, and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over an article by Thrift entitled "Java Enabled Television", in view of Gong (US 6,047,377) and Ahmad (US 5,925,127).

Claims 1-3, 7, 9, 11, 14, 15, and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thrift in view of Gong.

Applicant respectfully traverses these rejections in view of the amended claims and the comments which follow.

Discussion of Amended Claims

Claims 1 is amended to specify that the data defining a condition of the receiver under which access to the receiver function by the software application is permitted is received by the receiver from a headend. Claim 1 is also amended to specify that the receiver receives information from the headend that defines a security policy for the software application which contains a set of permissions for said software application. Corresponding amendments are made to apparatus claim 17 (see, e.g., Applicant's specification, page 13, lines 6-17 and Figure 1).

Claims 10 and 16 are cancelled.

Discussion of Rejection in View of Ellis and Macrae

Claims 1-6, 8, 10, 12, 13, 16, and 17 stand rejected as being unpatentable over Ellis in view of McRae.

Ellis discloses a program guide system which supports an interactive program guide and multiple non-guide applications, such as an Internet browser application, video-on-demand, electronic shopping, banking, and wagering, and the like (Col. 2, lines 1-15). The program guide application allows parents to lock programs using parental control resource 68a (Col. 6, lines 20-24). A program guide interface 54 allows non-guide applications to use program guide resources 68 or to use device resources 66 directly (Col. 6, lines 39-42).

MacRae discloses a mechanism for parents to define a table or matrix that is stored by a tuner in order to determine what channels are allowed to be tuned to, which can include the time of day, date, or other restrictions (Col. 4, lines 54-57). The disclosure of MacRae is a description of how parental ratings and other types of parental control for television viewing is accomplished on most televisions and set-top boxes by user control.

Applicant's claimed invention provides a dynamic security system in which the headend (network provider) specifies a security policy for software applications present at the receiver. Applicant's claimed security method controls what a software application is allowed to do, which is defined by the permissions of the security policy, and when (under what conditions) the software application is allowed to do what is permitted, which is defined by the current state of the receiver. Data defining a condition of the receiver under which access to a receiver function by the software application is permitted is sent from the head end to the receiver. The headend also sends information to the receiver which defines a security policy for the receiver. The security policy contains a set of permissions for the software application. When the receiver receives a control signal requesting access to a receiver function upon execution of the software application, a determination is made as to whether the security policy contains a permission for the software application to access the receiver function. If so, the current state of the receiver is checked against the data defining a condition of the receiver under which the receiver function may be accessed. If the condition is met, the software application is allowed to access the receiver function. If the condition is not met, the software application is not allowed to access the receiver function. If the security policy does not contain a permission for the software application to access the receiver function, access to the receiver function is prevented.

Therefore, Applicant's invention sets forth methods and apparatus for establishing a dynamic security system. Applicant's system is dynamic in that it is dependent on the current state of the receiver, which can change at any time. In addition to checking for the required permission to access the receiver function, data defining a condition of the receiver under which access to the receiver function by the software application is permitted is checked against data defining the current state of the receiver. Such a system provides for greater control than that which can be achieved using static or predefined conditions. For example, with Applicant's invention, if a user is not allowed to watch a football game because he lives in an area that has been blacked out by the network for this game, the associated application at the receiver which shows the related sports statistics for the game will not be able to execute.

Ellis does not disclose the use of any type of security policy by which the headend controls how applications are run at the terminal or how applications are allowed to access resources or functions of the terminal based on those security policies and related conditions of the terminal. Ellis does not disclose or remotely suggest the use of both permissions and conditions from the headend as claimed by Applicant. In particular, the EPG application with parental control of Ellis relied on by the Examiner does not have an associated security policy which contains a permission for the software application to access the receiver, as claimed by Applicant. Also, in Ellis there is no comparison between data defining a condition of the receiver under which access to the receiver function by the software application is permitted, which is received from the headend, and data indicative of a current state of the receiver. In Ellis, the parental control is a user defined control which prevents a user from viewing a program, rather than a headend defined control which prevents a software program from accessing a receiver function, as claimed by Applicant.

Further, the application guide interface of Ellis merely manages what program guide resources can be accessed by non-program guide applications which are running simultaneously, which may result in conflicting requests to use certain resources (i.e., display, database, tuner, etc.). These conditions (when a non-guide application can access a guide resource) are predefined static conditions which are not dependent (i.e., do not change) on a current state of the receiver.

Further, the Examiner has also acknowledged that Ellis does not disclose Applicant's step of "determining whether said condition of the receiver is met by data indicative of a current state of the receiver" (Office Action, page 6). The Examiner relies on MacRae as disclosing this subject matter.

Macrae, like Ellis, does not discuss or disclose security policy information provided from a headend to the receiver which contains permissions for a software application at the receiver. Macrae also doe not disclose or remotely suggest a receiver which receives data defining a condition of the receiver under which a receiver function may be accessed, as claimed by Applicant.

In Macrae, the tuner may be controlled by user inputs for parental rating limits, time of day, channel numbers and the like, to limit access to certain channels or content. The system of Macrae is not a headend defined security system having a security policy with associated permissions and data defining a condition under which a receiver function may be accessed by a software application, which are both provided by the headend to the receiver.

As discussed above, the present invention advantageously uses a dynamic approach to providing access control for software applications. Unlike the present invention in which the end user and the content provider are both protected, with rating control schemes such as that disclosed in MacRae, only the end user is protected. With such prior art rating control, the end user is in charge of defining the security policy that applies (e.g., setting the conditions, rating ceiling and the password). In contrast, with the present invention, the network's service provider (headend) is in charge of defining the policy to protect the different content providers that are on the network. Prior art rating control schemes such as MacRae are static systems, since the channel is either always locked (the user does not have the password) or always accessible (the user has the password). Such systems are not dependent on the current state of the receiver, as is Applicant's claimed system.

For example, with the present invention, the same application may run on certain channels but will not run on others, e.g., when the user tunes to another channel (thereby changing the current condition), sometimes the application stays on, and sometimes it is terminated, depending

on the permissions of the security policy. In the prior art rating mechanism, changing channels really means switching applications (considering a video channel an application). The present invention can accommodate multiple simultaneous applications (e.g., a data application running on top of a video channel), where changing channels sometimes leaves the same data application on, and sometimes does not, based on the security policy and the current state of the receiver (see, e.g., Applicant's specification, page 30, line 22 through page 32, line 22).

Such advantages are not provided by the disclosures of Ellis or MacRae, taken alone or in combination. A combination of Ellis and Macrae such as suggested by the Examiner would only results in a user defined parental rating control system (as disclosed in Macrae) with an associated program guide application having an interface which controls access to program guide resources by non-guide applications (as disclosed in Ellis).

As neither Ellis nor MacRae disclose or remotely suggest:

(a) receiving data at the receiver from a headend, said data defining a condition of the receiver under which access to the receiver function by the software application is permitted;

(c) receiving information at the receiver from the headend, said information defining a security policy for said software application which contains a set of permissions for said software application;

(c) determining whether the security policy for an application contains a permission to access a receiver function, and

(d) determining whether the condition of the receiver is met by data indicative of a current state of the receiver.

Therefore, the combination of Ellis and MacRae would not have led one skilled in the art to Applicant's invention as suggested by the Examiner.

Discussion of Rejection in View of Thrift, Gong, and Ahmad

Claims 1 -3, 7, 9, 11, 14, 15 and 17 stand rejected as being unpatentable over Thrift in view of Gong and Ahmad.

Thrift describes the use of Java applets in a television environment. However, as acknowledged by the Examiner, Thrift does not address any security issues associated with the use or downloading of such applets.

The Examiner relies on Gong as disclosing "a method and apparatus for establishing and maintaining security rules in conjunction such as that utilized by received and executed 'software applications' such as those associated with the JAVA ™ programming language in order to control television 'receiver functions'" (Office Action, page 3). Gong does disclose a Java security architecture which uses permissions to manage and control code executed by a computer system. Applicant respectfully submit that the present invention is an extension of the Java security architecture disclosed in Gong. Applicant has referred to an article by Gong entitled "Java Security Architecture" referenced on page 4, lines 11-13 of Applicant's specification, which essentially summarizes the disclosure of the Gong patent. Applicant's disclosure at pages 4-6 discusses how the present invention extends the security architecture provided by Gong.

Gong does not disclose or remotely suggest using conditions corresponding to the current state of the receiver in connection with permissions for controlling an application's access to a function of the receiver, as claimed by Applicant. With Applicant's claimed invention, it is determined whether the security policy for a software application contains a permission for the software application to access the receiver function. In addition, data defining a condition of the receiver under which access to the receiver function by the software application is permitted is provided to the receiver from the headend. If the security policy for the software application contains the permission, then it will be determined whether the condition of the receiver is met by data indicative of the current state of the receiver. In Applicant's system, both the permission must be present and the current state of the receiver must satisfy the condition before the software application can access the receiver function. Therefore, Applicant's security system is dynamic, in that it is dependent on the current state of the receiver, which can change frequently. In contrast to Applicant's invention, Gong merely provides static permissions for accessing functions of a receiver in which a permission specified in a security policy is compared against a

permission requested by an application, and does not disclose the use of additional conditions related to the state of the receiver in connection with the permissions.

The Examiner has cited to Col. 16, lines 47-55 of Gong as disclosing the use of conditions as claimed by Applicant (Office Action, page 4). The cited passage of Gong mentions that a bank account permission may have an action, an account, and a maximum amount attribute. The action, account, and maximum amount are part of the permission or instructions (Col. 16, lines 9-22), and are not a condition of the receiver as claimed by Applicant. As set forth, for example, in Applicant's claims 1-6, the condition claimed by Applicant may be: a conditional access state of the receiver, such as a blackout state, a pay-per-view state, or an authorization state; a user state, which may be defined by a user preference, a user password, or a user identifier; time, date, or day, or the like.

Gong does not disclose a dynamic security system as is provided by the present invention. For example, an ABC application may come with a policy that it can be run at the set-top box only if it is authorized for the ABC services (e.g., ABC television channel). This is a static security policy. The box is either authorized or it is not. It is very easy to determine the authorization state of the box when evaluating this permission and it will always come back with the same answer. If an additional condition is added, such that the box must also be tuned to the ABC channel while running the ABC application (e.g., to make sure that the box is not running the CNN stock ticker application while tuned to BBC news), the evaluation of the permission to run the ABC application will come back with different answers depending on what channel the box is tuned to. In other words, the security of the present invention is dynamic in the sense that it is dependent on the current state of the receiver, which can change.

The Examiner has indicated that is unclear as to whether Gong discloses conditions which are related to a current state of the receiver (Office Action, page 9). The Examiner relies on Ahmad as disclosing the use of conditions relating to a current state of the receiver as claimed by Applicant (Office Action, page 9).

Ahmad discloses a system for monitoring the use of a rented software program which provides a Software Monitor that keeps track of how long or how many times a program has

been used and compares it to a user license to make sure the original conditions (i.e., total rental time or number of uses allowed) have not been exceeded (Abstract).

The system of Ahmad is not tied to a current state of a digital television receiver, as claimed by Applicant. Instead, Ahmad defines static (predefined) conditions that are monitored by a Software Monitor, rather than a dynamic condition derived from a current state of the receiver. The number of times an application has been accessed is not equivalent to a current state of the receiver.

For example, an equivalent case of a dynamic condition in the system of Ahmad would be for the rental agreement to specify that the program can be used for five days, but only if another program was not used at the same time. The Software Monitor of Ahmad would then have to check not only the rental time to determine authorized use (a premission), but also all other programs running on the computer to determine whether they are permitted to be used at the same time in accordance with the original license (a current state of the receiver checked against data defining the conditions under which the function can be accessed). However, Ahmad does not disclose or suggest such a mechanism.

Applicant respectfully submits that the present invention would not have been obvious to one skilled in the art in view of the combination of Thrift, Gong and Ahmad. None of the cited references discloses a system which checks both for a permission and for a current condition of the receiver to match data defining a condition of the receiver under which the receiver function can be accessed (which is a dynamic condition).

In particular, the combination of Thrift, Gong, and Ahmad does not disclose or remotely suggest receiving data at a receiver from a headned defining a condition of the receiver under which access to the receiver function by the software application is permitted, receiving information at the receiver from the headend defining a security policy for the software application which contains a set of permissions for the software application, determining if a security policy for the software application contains a permission for the software application to access the receiver function, and if the permission is present, determining whether the condition of the receiver is met by data indicative of a current state of the receiver, as claimed by Applicant.

Response to Rejections Based on Thrift in View of Gong

Claims 1-3, 7, 9, 11, 14, 15, and 17 stand rejected as being unpatentable over Thrift in view of Gong.

Thrift describes the use of Java applets in a television environment. However, as acknowledged by the Examiner, Thrift does not address any security issues associated with the use or downloading of such applets.

Gong discloses a Java security architecture which uses permissions to manage and control code executed by a computer system. Gong compares a permission specified in a security policy and a permission requested by the application (or applet or showlet). These two permissions are statically compared to see whether the permission from the security policy implies the permission from the application request to determine whether the requested action is authorized. Applicant's present invention adds a new step to the method disclosed in Gong, namely checking the current state of the receiver against data defining a condition under which access to a receiver function may be permitted to determine whether the requested action (access to the requested receiver function) is authorized or not. With Applicant's invention, the data defining the condition under which access to the receiver function can be permitted is provided from the headend.

Gong does not disclose or remotely suggest using conditions corresponding to the current state of the receiver in connection with permissions for controlling an application's access to a function of the receiver, as claimed by Applicant. In Applicant's system, both the permission must be present and the current state of the receiver must satisfy the condition before the software application can access the receiver function. Therefore, Applicant's security system is dynamic, in that it is dependent on the current state of the receiver, which can change frequently. In contrast to Applicant's invention, Gong merely provides static permissions for accessing functions of a receiver, and does not disclose the use of additional conditions in connection with the permissions, as claimed by Applicant.

Applicant respectfully submits that the present invention would not have been obvious to one skilled in the art in view of the combination of Thrift and Gong, as neither of the cited references discloses or remotely suggests the features of Applicant's claims 1 and 17. In particular, the combination of Thrift and Gong does not disclose or remotely suggest providing data at the receiver from the headend which defines a condition of the receiver under which access to the receiver function by the software application is permitted, determining if an associated security policy of the software application contains a permission for the software application to access the receiver function, and if the permission is present, determining whether a condition of the receiver is met by data indicative of a current state of the receiver, as claimed by Applicant.

Applicant respectfully submits that the present invention would not have been obvious to one skilled in the art in view of the combination of Thrift and Gong, or any of the other references of record.

Further remarks regarding the asserted relationship between Applicant's claims and the prior art are not deemed necessary, in view of the above discussion. Applicant's silence as to any of the Examiner's comments is not indicative of an acquiescence to the stated grounds of rejection.

Withdrawal of the rejections under 35 U.S.C. § 103(a) is therefore respectfully requested.

Conclusion

In view of the above, the Examiner is respectfully requested to reconsider this application, allow each of the presently pending claims, and to pass this application on to an early issue. If there are any remaining issues that need to be addressed in order to place this application into condition for allowance, the Examiner is requested to telephone Applicant's undersigned attorney.

Respectfully submitted,

Douglas M. McAllister
Attorney for Applicant(s)
Registration No. 37,886
Law Office of Barry R. Lipsitz
755 Main Street
Monroe, CT 06468
(203) 459-0200

Attorney Docket No.: GIC-535
Date: August 18, 2004